



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/723,403

11/26/2003

Jeffrey B. Lotspiech

ARC920030090US1

7944

67232

7590

02/20/2008

CANTOR COLBURN, LLP - IBM ARC DIVISION

20 Church Street

22nd Floor

Hartford, CT 06103

EXAMINER

WANG, HARRIS C

ART UNIT

PAPER NUMBER

2139

MAIL DATE

DELIVERY MODE

02/20/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/723,403	<b>Applicant(s)</b> LOTSPIECH ET AL.	
	<b>Examiner</b> HARRIS C. WANG	<b>Art Unit</b> 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 05 December 2007.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-8, 17-24 and 33-40 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-8, 17-24 and 33-40 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 November 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

1.

Claims 1-8, 17-24, 33-40 are pending

Claims 9-16, 25-32, 41-48 have been cancelled

### ***Response to Arguments***

Applicant's arguments with respect to claims 1-8, 17-24, 33-40 have been considered but are considered unpersuasive.

The Applicant argues that the combined teachings do not teach the newly amended claimed limitation "wherein the physical media includes a physical media unique key encrypted in each of the keys such that (a) a media key obtained from the media key block is combined with a volume identifier (ID) for the physical media using a cryptographic hash to provide the physical media unique key, and the physical media unique key is then encrypted in each of the corresponding content keys; or (b) wherein the physical media unique key is the media key."

The Examiner's main reference Pestoni discloses the newly amended limitations. Page 11 of Pestoni shows a "media key" obtained from the media key block and combined with a volume identifier (ID) using a cryptographic hash (one-way function) to provide the physical media unique key ( $K_{mu}$ ), and the physical media key is encrypted in the content keys ( $E_{K_{mu}}(K_t)$ )

Therefore the Examiner finds the arguments unpersuasive.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-5, 8, 17-21, 24, 33-37 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pestoni in view of Akishita further in view of Sims .

Regarding Claims 1, 17 and 33

Pestoni teaches a method for delivering multimedia content on a physical media, comprising:

placing at least one media key block on the physical media (*pg. 11, the Figure shows the Media Key Block on the physical media*);

encrypting the encryption key with a key derived from the media key block (*pg. 11,  $E_{Kmu}(Kt)$ , where  $E_{Kmu}$  is the key derived from the media key block, and  $Kt$  is the encryption key*)

delivering the encrypted encryption key to a player of the physical media (*pg. 11,  $E_{Kmu}(Kt)$  is shown being delivered to the player where it is decrypted.*)

selecting a media key block from a set of media key blocks (*pg. 10, "All elements must be licensed from licensing center (License Management International, LLC)...MKBs- To*

*CPRM-enable media") It is inherent that one MKB is selected from the group of MKBs provided by the licensing center.*

Wherein the physical media includes a physical media unique key encrypted in each of the content keys such that (a) a media key obtained from the media key block is combined with a volume identifier (ID) for the physical media using a cryptographic hash to provide the physical media unique key, and the physical media unique key is then encrypted in each of the corresponding content keys (*pg. 11 of Pestoni shows a "media key" obtained from the media key block and combined with a volume identifier (ID) using a cryptographic hash (one-way function) to provide the physical media unique key (Kmu), and the physical media key is encrypted in the content keys (Ekm(Kt))* )

Pestoni does not teach dividing the multimedia content on the physical media into multiple parts, each part being encrypted with a different encryption key. Akishita teaches encrypting multiple sectors of a DVD with multiple content keys (*Fig. 27 a-b, "multiple content keys...serving as encryption keys corresponding to sectors...are encrypted and stored in the security header configured corresponding to the contents" Paragraph [0489]*)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Pestoni to divide the physical media into multiple parts and encrypt each part with a different encryption key.

The motivation is to allow different parts of a physical medium to have multiple encryptions, instead of just having one key to encrypt the entire disc.

Pestoni and Akishita do not further teach randomly selecting content keys corresponding to each part of the multimedia content

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Pestoni and Akishita with the feature of randomly selecting content keys.

The prior art Pestoni included each element claimed (physical media, media key block, content key) and one of ordinary skill in the art could have combined the elements as claimed by known methods (dividing the physical media into multiple parts and encrypting each part with a different encryption key, as taught by Akishita, and randomly selecting content keys, as taught by Sims) and that in combination, each element merely would have performed the same function as it did separately. One of ordinary skill in the art would have recognized that the results of the combination were predictable.

Regarding Claim 2, 18 and 34

Pestoni, Akishita and Sims teach the method of claim 1, wherein in CPRM inherently requires delivering the encrypted encryption key comprises delivery over a network.

Regarding Claims 3-5, 19-21 and 35-37

Pestoni, Akishita and Sims teach the method of claim 1, wherein the encrypted encryption key is associated with a price related to the use of the part. Pestoni in Pg. 10 writes “small fees [are] associated with the keys and MKBs.” It is inherent that the price is determined when the encrypted encryption key is delivered.

Regarding Claim 8, 24 and 40

Pestoni, Akishita and Sims teach the method of claim 2. Pestoni and Akishita do not explicitly teach wherein the delivery over the network involves a secure protocol; and further comprising placing necessary data for the secure protocol on the physical media.

It would have been obvious to one of ordinary skill in the art at the time of the invention to make the delivery of the keys over the network involve a secure protocol and further comprising the physical media having necessary data for the secure protocol.

The motivation is that the delivery of keys requires security, where secure network transfers are well known in the art.

Claims 6-7, 22-23 and 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pestoni, Akishita and Sims as applied to claim 1-5 above, and further in view of Husemann (US 20050100161).

Regarding Claims 6-7, 22-23 and 38-39

Pestoni, Akishita and Sims teach teach the method of claim 3. Pestoni and Akishita do not explicitly teach further comprising associating the encrypted encryption key with a maximum price, and preventing playback once the maximum price is reached.

Huseman (Paragraph [0037]) teaches “the clearinghouse will charge the customer’s registered credit card, encapsulate the requested content keys...and return the set of encapsulated keys.”

It would have been obvious to one of ordinary skill in the art at the time of the invention to associate a maximum price with the key, and prevent playback once the maximum price is reached.

The motivation is that the server protects itself from those with bad credit history by assigning a maximum price, which the Examiner interprets as a credit limit, so that if there is no credit left, no transaction will take place.

### ***Conclusion***



Any inquiry concerning this communication or earlier communications from the examiner should be directed to HARRIS C. WANG whose telephone number is (571)270-1462. The examiner can normally be reached on M-F 9-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KRISTINE KINCAID can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139